Guia docent
300049 - SX - Seguretat en Xarxes

Última modificació: 31/05/2021

Unitat responsable: Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels
Unitat que imparteix: 744 - ENTEL - Departament d'Enginyeria Telemàtica.

Titulació: GRAU EN ENGINYERIA TELEMÀTICA (Pla 2009). (Assignatura obligatòria).

Curs: 2021 **Crèdits ECTS:** 4.0 **Idiomes:** Català, Castellà, Anglès

PROFESSORAT

Professorat responsable: Definit a la infoweb de l'assignatura.

Altres:

CAPACITATS PRÈVIES

- Coneixements de programació.
- Coneixements bàsics del sistema Unix/Linux.
- Coneixements bàsics de xarxes.
- Saber diferenciar els diferents aspectes que implica la comunicació de dades. És a dir, tenir una comprensió clara del funcionament dels models de capes OSI y TCP/IP.

REQUISITS

Cap

COMPETÈNCIES DE LA TITULACIÓ A LES QUALS CONTRIBUEIX L'ASSIGNATURA

Específiques:
1. CE 22 TEL. Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones de telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y telegráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos. (CIN/352/2009, BOE 20.2.2009)

Genèriques:
7. GESTIÓN DE PROYECTOS - Nivel 2: Definir els objectius d'un projecte ben definit, d'abast reduït, i planificar-ne el desenvolupament, determinant els recursos necessaris, tasques a realitzar, repartiment de responsabilitats integració. Utilitzar adequadament eines de suport a la gestió de projectes.

Transversals:
2. COMUNICACIÓ EFICAÇ ORAL I ESCRITA - Nivell 1: Planificar la comunicació oral, respondre de manera adequada les qüestions formulades i redactar textos de nivell bàsic amb correcció ortogràfica i gramatical.
3. COMUNICACIÓ EFICAÇ ORAL I ESCRITA - Nivell 2: Utilitzar estratègies per preparar i dur a terme les presentacions orals i redactar textos i documents amb un contingut coherent, una estructura i un estil adequats i un bon nivell ortogràfic i gramatical.
4. COMUNICACIÓ EFICAÇ ORAL I ESCRITA - Nivell 3: Comunicar-se de manera clara i eficient en presentacions orals i escrites adaptades al tipus de públic i als objectius de la comunicació utilitzant les estratègies i els mitjans adequats.
5. COMUNICACIÓ EFICAÇ ORAL I ESCRITA: Comunicar-se de forma oral i escrita amb altres persones sobre els resultats de l'aprenentatge, de l'elaboració del pensament i de la presa de decisions; participar en debats sobre temes de la pròpia especialitat.
6. EMPRENEDORIA I INNOVACIÓ - Nivell 3: Utilitzar coneixements i habilitats estratègiques per a la creació i gestió de projectes, aplicar solucions sistèmiques a problemes complexos i dissenyar i gestionar la innovació en l'organització.

METODOLOGIES DOCENTS

Fonamentalment, és una assignatura orientada a l'estudi, esforç, treball i avaluació individual de l'estudiant.
Les classes de teoria són, fonamentalment, classes d'explicació per part del professor a la pissarra i amb transparències, tot i així s'incentiva la participació de l'estudiant a la classe fomentant les preguntes i comentaris.
Les transparències de cada classe estan disponibles a ATENEA, al menys una setmana abans d'explicar pel professor; l'alumne pot i ha de dur-les a la classe impreses per fer-hi les anotacions pertinents.
Quant a les activitats dirigides, el professor fa classes per encaminar l'alumne, que continua el treball de manera autònoma. La resta de classes s'utilitzaran per al seguiment i/o ajuda de l'activitat a desenvolupar pels alumnes.

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

Un cop acabada l'assignatura de Seguretat en Xarxes, un estudiant ha de ser capaç de:
- Entendre quins aspectes engloba la seguretat en xarxa sabent identificar els potencials atacs i els possibles sistemes per a evitar-los.
- Identificar i comprendre els algoritmes criptogràfics més utilitzats per dotar de seguretat a les xarxes.
- Definir els diferents mètodes de confidencialitat, integritat, autenticació, actualitat i gestió del material criptogràfic.
- Conèixer diferents sistemes de seguretat perimètrica, com ara tallafocs i sistemes de detecció d'intrusos
- Utilitzar els diferents protocols de seguretat per als intercanvis de dades a Internet: seguretat IP, xarxes privades virtuals, mecanismes de seguretat per al correu electrònic, seguretat a la www o sistemes segurs de pagament.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores activitats dirigides	16,0	16.00
Hores grup gran	24,0	24.00
Hores grup mitjà	4,0	4.00
Hores aprenentatge autònom	56,0	56.00

Dedicació total: 100 h

CONTINGUTS

1. INTRODUCCIÓ A LA SEGURETAT EN XARXA

Descripció:
Conceptes fonamentals. La seguretat en xarxa engloba: atacs de seguretat, mecanismes de seguretat i serveis de seguretat. A partir del coneixement d'aquests tres blocs, es planteja un model de seguretat en xarxa que ha d'estar present durant tota l'assignatura.
Els mecanismes i serveis de seguretat es basen, en gran mesura, en eines que garanteixin confidencialitat, integritat, autenticació, AAA, no rebuig i anonimat.

Activitats vinculades:
Examen parcial, examen final

Dedicació: 4h 15m
Grup gran/Teoria: 2h
Grup mitjà/Pràctiques: 0h 15m
Aprenentatge autònom: 2h

2. EINES DE SEGURETAT DE LA INFORMACIÓ

Descripció:
Aritmètica modular i criptografia clàssica (2h)
Criptografia simètrica moderna (4h)
- Xifrat de flux/bloc
- Modes de funcionament xifradors de bloc (ECB, OFB, CBC, CTR, CBC-MAC, CCM, etc.)
Criptografia asimètrica i PKI
- Intro: funcions asimètriques/unidireccionals i criptografia asimètrica
- RSA
Necessitat d'autenticar:
- PKI: certificats digitals, firma electrònica
- Secret compartit: Message Authentication Codes (MAC)
Gestió i acord de claus

Activitats vinculades:
Examen parcial, examen final

Dedicació: 33h 45m
Grup gran/Teoria: 10h 30m
Grup mitjà/Pràctiques: 1h 15m
Aprenentatge autònom: 22h

3. RESUMEN AMENACES I CONTRAMESURES

Descripció:
Anàlisi de les principals amenaces a la seguretat en xarxes així com resum de les contramesures a l'estat de l'art.

Activitats vinculades:
Examen parcial, examen final, AD3

Dedicació: 11h 15m
Grup gran/Teoria: 2h
Grup mitjà/Pràctiques: 0h 15m
Activitats dirigides: 2h
Aprenentatge autònom: 7h

4. PROTOCOLS DE SEGURETAT A INTERNET

Descripció:
Seguretat aplicada a xarxes, protocols de seguretat a nivell d'enllaç (p. ex. WEP, WPA), a nivell de xarxa (IPSec) i transport (SSL/TLS, SSH).

Activitats vinculades:
Examen parcial, examen final, AD1, AD2

Dedicació: 50h 45m
Grup gran/Teoria: 9h 30m
Grup mitjà/Pràctiques: 2h 15m
Activitats dirigides: 14h
Aprenentatge autònom: 25h

ACTIVITATS

AD1. Virtuaització de xarxes, atacs de MITM a nivell d'enllaç i xarxes privades virtuals amb IPSec

Descripció:
Implementació d'escenaris de xarxa virtualizados així com de l'encaminament per garantir les connectivitats necessàries.
Implementació d'atacs de man-in-the-middle (MITM) a nivell d'enllaç.
Implementació d'una xarxa privada virtual (VPN) basada en IPSec.

Objectius específics:
Com a activitat d'avaluació, l'objectiu és demostrar el grau d'aprenentatge i consolidació de coneixements pràctics de laboratori obtingut durant el període previ corresponent

Material:
Indicacions del professor, Internet, els propis resultats obtinguts durant la seva realització

Lliurament:
Presentació d'una memòriai defensa del sistema implementat davant el professor. Qüestionari individual

Dedicació: 16h
Grup gran/Teoria: 2h
Activitats dirigides: 7h
Aprenentatge autònom: 7h

AD2. AUTORITATS DE CERTIFICACIÓ, SSL/TLS i SSH

Descripció:
Implementació d'una autoritat de certificació i per al seu ús en l'escenari IPSec desenvolupat en la AD1.
Implementació d'atacs a SSL/TLS basats en l'atac MITM de AD1
Implementació dels tres tipus de forwarding SSH

Objectius específics:
Com a activitat d'avaluació, l'objectiu és demostrar el grau d'aprenentatge i consolidació de coneixements pràctics de laboratori obtingut durant el període previ corresponent

Material:
Indicacions del professor, Internet, els propis resultats obtinguts durant la seva realització.

Lliurament:
Presentació d'una memòria i defensa del sistema implementat davant el professor. Qüestionari individual

Dedicació: 17h
Grup gran/Teoria: 2h
Activitats dirigides: 7h
Aprenentatge autònom: 8h

AD3. ACTIVITAT OBERTA

Descripció:
En funció del desenvolupament del curs i de les inquietuds dels alumnes, es proposarà una activitat dirigida

Objectius específics:
Com a activitat d'avaluació, l'objectiu és demostrar el grau d'aprenentatge i consolidació de coneixements pràctics de laboratori obtingut durant el període previ corresponent.

Material:
Indicacions del professor, Internet, els propis resultats obtinguts durant la seva realització

Lliurament:
Presentació d'una memòria i defensa del sistema implementat davant el professor. Qüestionari individual

Dedicació: 8h
Activitats dirigides: 2h
Aprenentatge autònom: 6h

PLANIFICACIÓ D'EXÀMENS (RESOLUCIÓ DE PROBLEMES)

Descripció:
2 classes d'hores abans de l'exàmen parcial i del final, que han de servir per orientar l'alumne per a ambdós exàmens.

Lliurament:
Problemes

Dedicació: 8h
Grup gran/Teoria: 4h
Aprenentatge autònom: 4h

Examen parcial

Dedicació: 4h 30m
Grup gran/Teoria: 1h 30m
Aprenentatge autònom: 3h

Examen final

Dedicació: 4h 30m
Grup gran/Teoria: 1h 30m
Aprenentatge autònom: 3h

SISTEMA DE QUALIFICACIÓ

S'aplicaran els criteris d'avaluació definits a la infoweb de l'assignatura.

NORMES PER A LA REALITZACIÓ DE LES PROVES.

L'assistència per a la defensa de les activitats dirigides és obligatòria. Les faltes hauran de ser justificades.